UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

COALITION FOR INDEPENDENT TECHNOLOGY RESEARCH,

Plaintiff,

v.

GREG ABBOTT, in his official capacity as Governor of the State of Texas, *et al.*,

Defendants.

Civil Action No. 1:23-cv-783

# SUPPLEMENTAL DECLARATION OF PROFESSOR BRUCE SCHNEIER

I, Bruce Schneier, declare:

1. I am submitting this declaration to supplement the declaration I submitted on September 7, 2023. I am familiar with the arguments Defendants have made in support of their motion to dismiss and opposition to the plaintiff's motion for a preliminary injunction, as well as with the declarations submitted by Meghan Frkuska and Richard Anderson. My declaration is based on expertise I have developed over the course of my academic study and professional practice related to computer security, national security, and public policy. I have personal knowledge of the facts set forth herein and, if called to testify as a witness, I could do so competently under oath.

## <u>The Chinese Government Does Not Need TikTok to Acquire Sensitive Data About American Users</u>

2. As I explained in my opening declaration, there are legitimate concerns about the Chinese government's ability to access data held by Chinese companies and their subsidiaries. For present purposes, however, the important point is that China does not need TikTok to acquire

sensitive data about Americans. It can easily purchase this information from data brokers, advertising aggregators, and other applications on the open market.[1] Banning TikTok in an effort to stop the Chinese government from gathering information of intelligence value on American users is like trying to dam a river with a single stone. Even if one accepts Texas's unsubstantiated claim that the Chinese government has unfettered access to TikTok's data, Texas offers no evidence that its ban will make it any harder for China to collect data about Texans, or to generate sophisticated insights about them. The critical question is: What could the Chinese government do with TikTok's data that it couldn't do without it? The answer: essentially nothing.

3. Texas has argued that TikTok engages in a form of keylogging that could give the Chinese government access to American users' passwords, private messages, and financial information. But nearly every application has the *capability* to log keystrokes. And while it would be remarkable if TikTok actually used that capability to collect and store users' passwords, private messages, and other sensitive information, Texas does not offer any evidence that TikTok has in fact done this, and I do not know of any such evidence. (Incidentally, if TikTok did log this kind of information in the future, independent researchers would certainly learn of this, and alert the public to it, right away—assuming, of course, that they had not been banned from conducting research using TikTok.) Notably, the only article Texas cites in support of its keylogging argument explains that the researcher who uncovered the keystroke tracking "was unable to ascertain whether keystrokes were actively being tracked, and whether that data was being sent to TikTok."[2]

4. I understand that Texas has also argued that TikTok can access users' cameras and microphones, creating the risk that the Chinese government could eavesdrop on American users.

[1] Schneier Decl. ¶¶ 24–30, ECF No. 20-3.

[2] Paul Mozur et al., *TikTok Browser Can Track Users' Keystrokes, According to New Research*, N.Y. Times (Aug. 19, 2022), https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html.

Here, too, what Texas states as fact more closely resembles speculative fiction. Given TikTok's affordances—which allow users to create short videos—it is not a surprise that TikTok would require access to a users' camera and microphone while the application is in use. But Texas points to no evidence that TikTok accesses these features when the application is not active or without users' consent, and I do not know of any such evidence.[3]

## **The Ban is Ineffective and Counterproductive in Addressing Concerns about Privacy**

5. I explained in my opening declaration that Texas's ban is ineffective in addressing concerns related to privacy because it does nothing to address the root of the issue: the intrusive data collection practices themselves.[4] Texas has interpreted my statements as suggesting that states should not be permitted to act to protect privacy unless they tackle all problems concerning data collection simultaneously. This misunderstands my position. My point is not that Texas and other states should not be permitted to take steps to protect users' privacy unless they address all harmful data collection practices at once; it is that Texas has not shown that banning TikTok does anything at all to actually protect users' privacy. In fact, the ban is worse than nothing, because restricting independent research about TikTok will have downstream, negative implications for privacy—as well as for security. Of course Texas should take steps to address user privacy, but surely it would be better if the steps it took were effective rather than counterproductive.

## **The Ban is Ineffective and Counterproductive in Addressing Concerns about Security**

6. As a further justification for its ban, Texas points to a number of high-profile hacks that have targeted government offices and resources. I have no doubt that hackers and foreign

[3] It bears noting that TikTok claims that "[t]he camera and microphone are only activated when a user has granted TikTok permission to access them. Otherwise, TikTok does not collect any information from these sources. Additionally, when the TikTok app is closed, it does not collect any information from these sources." *TikTok Truths: A new series on our privacy and data security practices*, TikTok Newsroom (Jun. 13, 2023), https://newsroom.tiktok.com/en-us/tiktok-truths-a-new-series-on-our-privacy-and-data-security-practices.

[4] Schneier Decl. ¶¶ 17–21.

governments are interested in compromising government systems. This is part of the reason why independent security research is so important. However, none of the examples provided by Texas involved TikTok. If anything, they prove the point I made in my opening declaration—that banning TikTok would not have any significant effect on the ability of malicious actors to break into or compromise Texas's networks.[5]

7. Texas's declarant Richard Anderson, who serves as the University of North Texas's (UNT) Chief Information Security Officer, confirms this. Anderson explained that the UNT system faces on average 12,049 phishing attacks and 75,753 network attacks each day, as well as 621 malware attacks each month.[6] But Anderson does not attribute any of these attacks to TikTok or the Chinese government, and there is no indication that banning TikTok would in any way reduce these numbers. The kinds of cybersecurity threats Anderson references—including ransomware attacks, SQL injections, and phishing schemes—have nothing to do with TikTok. TikTok was not the vector for any of these attacks, nor does Texas offer any evidence that it is especially likely to be a vector for attacks in the future.

## **Providing Dedicated IT Resources is a Viable Alternative to a Categorical Ban**

8. As I noted in my opening declaration, public universities could address security concerns by issuing dedicated devices to faculty engaged in TikTok-related research and by establishing dedicated networks for the use of TikTok in research and teaching.[7] If Texas's aim is to insulate state IT resources from cybersecurity threats, providing faculty with dedicated devices and a dedicated network would broadly accomplish this aim without impairing important research and teaching.

[5] Schneier Decl. ¶¶ 36–37.

[6] Anderson Decl. ¶¶ 11–13, ECF No. 31-2.

[7] Schneier Decl. ¶ 49.

9. As I noted in my opening declaration, setting up dedicated devices and a dedicated network would be trivial.[8] Network segmentation and segregation are standard cybersecurity practices and do not require specialized equipment or expertise. Nor would it be particularly costly to a university to issue a handful of dedicated computers or phones to those faculty engaged in research and teaching related to TikTok. Texas's declarant Richard Anderson, UNT's Chief Information Security Officer, offers no explanation for why such an accommodation would be burdensome or ineffective.

10. Texas has argued that faculty using state-provided dedicated networks and devices would still be handing over their personal information to TikTok. But faculty are handing over their information under the current regime, too. As I explained in my opening declaration, the ban does not prevent TikTok from collecting data about state employees if people in their social or professional networks use TikTok, or if they access third-party websites that utilize a TikTok tracking pixel.[9] Moreover, if faculty conduct TikTok-related research on their personal devices, as Texas contends they can (so long as those devices do not connect to the state network), this, too, will entail sharing data with TikTok. Texas's ban does not actually prevent TikTok from collecting information about faculty.

11. I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

Bruce Schneier

November 3, 2023

[8] *Id.*

[9] Schneier Decl. ¶¶ 19–20.